Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

1B04/51976

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

03103686.6

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Europäisches Patentamt | European Patent Office | Office européen des brevets

Anmeldung Nr:
Application no.: 03103686.6
Demande no:

Anmeldetag:
Date of filing: 06.10.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Verfahren und Schaltung zum Identifizieren und/oder Überprüfen von Hardware und/oder Software einer Vorrichtung und von einem mit der Vorrichtung zusammenwirkenden Datenträger

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G06F1/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

Verfahren und Schaltung zum Identifizieren und/oder Überprüfen von Hardware und/oder Software einer Vorrichtung und von einem mit der Vorrichtung zusammenwirkenden Datenträger

Die Erfindung bezieht sich auf ein Verfahren zum Identifizieren und/oder Überprüfen von Hardware und/oder Software einer Vorrichtung und von einem mit der Vorrichtung zusammenwirkenden Datenträger.

Die Erfindung bezieht sich weiters auf eine Schaltung zum Identifizieren und/oder Überprüfen von Hardware und/oder Software einer Vorrichtung und von einem mit der Vorrichtung zusammenwirkenden Datenträger.

Die Erfindung bezieht sich weiters auf eine eine derartige Schaltung beinhaltende Vorrichtung.

Im Zusammenhang mit der Identifizierung und/oder Überprüfung von Hardware und/oder Software einer Vorrichtung oder von einem Datenträger, der mit der Vorrichtung zusammenwirkt, wird es zunehmend wichtiger, elektronische Daten, die in der Vorrichtung oder in dem Datenträger gespeichert sind oder die zwischen dem Datenträger oder der Vorrichtung kommunizierbar sind, vor einem nicht autorisierten Zugriff zu schützen.

Derartige Daten können beispielsweise in einem PC, einem CD-Player, einem DVD-Player, einem Fernsehgerät, einem Mobiltelefon oder PDA gespeichert oder verwendet werden, wobei diese Vorrichtungen Hardware und/oder Software beinhalten, welche vor einem unberechtigten Zugriff zu schützen sind/ist. In diesem Zusammenhang ist es bekannt, derartige gegebenenfalls unsichere Vorrichtungen beispielsweise durch ein sogenanntes Trusted Platform Module (TPM) zu schützen. Dabei wird der Hauptprozessor bzw. die zentrale Recheneinheit einer derartigen zu schützenden Vorrichtung nur durch Verwendung eines derartigen TPM auf die Integrität seiner Hauptkomponenten überprüft, so dass dies beispielsweise das Einbringen von Viren oder Trojanischen Pferden verhindern kann.

Darüber hinaus ist es im Zusammenhang mit Lesevorrichtungen für externe Datenträger, beispielsweise für eine SmartCard, bekannt, eine Überprüfung im Bereich der Kommunikation zwischen der SmartCard und der zentralen Recheneinheit einer derartigen Lesevorrichtung zur Verfügung zu stellen, wobei beispielsweise ein sogenanntes Secure Application Module (SAM) verwendet wird, welches eine Überprüfung der beispielsweise auf einer SmartCard vorhandenen Autorisierungsdaten vor einem Weiterleiten von auf der SmartCard gespeicherten externen Daten an die zentrale Recheneinheit der Vorrichtung ermöglicht.

Um sowohl ein Überprüfen und/oder ein Identifizieren der Hardware und/oder Software der zentralen Recheneinheit als auch ein Überprüfen bzw. ein Identifizieren oder Autorisieren von einem in Bezug auf die Vorrichtung externen Datenträger, beispielsweise einer SmartCard, zu ermöglichen, wurde vorgeschlagen, sowohl beispielsweise ein TPM als auch ein SAM über jeweilige Interfaces mit der zentralen Recheneinheit bzw. dem Hauptprozessor der Vorrichtung zu kombinieren, wie dies beispielsweise aus dem Dokument US 2002/0134837 A1 zu entnehmen ist.

Derartige bekannte Konstruktionen unter Verwendung von zwei getrennten Modulen bzw. Chips für das TPM und das SAM haben sich als nachteilig erwiesen, da eine Kommunikation beispielsweise zwischen dem TPM und dem SAM nur über die zentrale Recheneinheit der Vorrichtung erfolgen kann. Insbesondere die Verbindungen zwischen den einzelnen Modulen und der zentralen Recheneinheit der Vorrichtung über entsprechende Interfaces und Leitungen hinweg sind darüber hinaus anfällig für Angriffe oder Manipulationen. Es wäre somit ein Leichtes eine Störung oder eine Beeinträchtigung der zu schützenden Vorrichtung zu bewirken und dabei die leicht angreifbare Verbindung zwischen den jeweiligen Modulen und der zentralen Recheneinheit als auch zwischen einem externen Datenträger und dem zwischengeschalteten SAM anzugreifen und derart die ordnungsgemäße Funktion der zu schützenden Vorrichtung zu beeinträchtigen und/oder einen nicht autorisierten Zugriff auf Daten in der Vorrichtung oder dem Datenträger zu erhalten. Darüber hinaus ist davon auszugehen, dass beispielsweise das TPM mit der zu schützenden Vorrichtung verbunden ist und somit nicht ohne weiteres bzw. lediglich unter Öffnung der Vorrichtung ersetzt werden kann. Weiters ist davon auszugehen, dass die verwendeten Module TPM und SAM gegebenenfalls über unterschiedliche Betriebssysteme verfügen und gegebenenfalls unterschiedliche Speicherkonfigurationen

und insbesondere unterschiedliche Verschlüsselungsalgorithmen verwenden, so dass ein unmittelbares Kommunizieren bzw. Verbinden, insbesondere für den Zweck eines Überprüfens und/oder Identifizierens von sicherheitsrelevanten Daten, wie beispielsweise Zutrittsdaten zwischen den einzelnen Modulen, nicht möglich ist. Weiters ist davon auszugehen, dass bei Verwendung von getrennten Modulen diesen jeweils verschiedene Identifikations-Codes bzw. ID-Codes zugewiesen werden bzw. werden müssen, so dass ein erhöhter Aufwand beispielsweise bei einer Initialisierung der einzelnen Bestandteile erforderlich ist.

Die Erfindung hat sich zur Aufgabe gestellt, ein Verfahren sowie eine Schaltung der eingangs genannten Art zu schaffen, bei welchen die vorstehenden angegebenen Nachteile vermieden sind.

Zur Lösung der vorstehend angegebenen Aufgabe umfasst ein Verfahren gemäß der Erfindung zum Identifizieren und/oder Überprüfen von Hardware und/oder Software einer Vorrichtung und von einem mit der Vorrichtung zusammenwirkenden Datenträger die folgenden Schritte:

Verfahren zum Identifizieren und/oder Überprüfen von Hardware und/oder Software einer Vorrichtung und von einem Datenträger, der zum Zusammenwirken mit der Vorrichtung vorgesehen ist, umfassend die folgenden Schritte:

Übertragen von ersten Autorisierungsdaten der Hardware und/oder Software an eine erste Einheit, Vergleichen der an die erste Einheit übertragenen ersten Autorisierungsdaten der Hardware und/oder Software mit in der ersten Einheit gespeicherten ersten Prüfdaten, Autorisieren der Hardware und/oder Software nach Feststellen einer Übereinstimmung zwischen den von der Hardware und/oder Software zur Verfügung gestellten ersten Autorisierungsdaten und den in der ersten Einheit gespeicherten ersten Prüfdaten, Übertragen von zweiten Autorisierungsdaten eines Datenträgers an eine zweite Einheit, Vergleichen der zweiten Autorisierungsdaten in der zweiten Einheit mit in der zweiten Einheit gespeicherten zweiten Prüfdaten, Autorisieren des Datenträgers bei einer Übereinstimmung zwischen den zweiten Autorisierungsdaten und den in der zweiten Einheit gespeicherten zweiten Prüfdaten, wobei ein direktes Datenaustauschen zwischen der ersten Einheit und der zweiten Einheit vorgenommen wird.

Zur Lösung der vorstehend angegebenen Aufgaben sind bei einer Schaltung gemäß der Erfindung zum Identifizieren und/oder Überprüfen von Hardware und/oder Software einer Vorrichtung und einem mit der Vorrichtung zusammenwirkenden Datenträger erfindungsgemäße Merkmale vorgesehen, so dass eine solche Schaltung gemäß der Erfindung auf die nachfolgend angegebene Weise charakterisierbar ist, nämlich:

Schaltung zum Identifizieren und/oder Überprüfen von Hardware und/oder Software einer Vorrichtung und von einem Datenträger, der zum Zusammenwirken mit der Vorrichtung vorgesehen ist, umfassend:

eine erste Einheit zum Identifizieren und/oder Überprüfen der Hardware und/oder Software der Vorrichtung, enthaltend eine zentrale Recheneinheit und wenigstens einen Speicher und ein Interface zu der zu identifizierenden und/oder zu überprüfenden Hardware und/oder Software, und eine zweite Einheit, enthaltend eine zentrale Recheneinheit und wenigstens einen Speicher und ein Interface zu einem externen Datenträger sowie ein Interface zu der Hardware und/oder Software, worin ein Kommunikations-Interface zwischen den zentralen Recheneinheiten der ersten Einheit und der zweiten Einheit vorgesehen ist.

Zur Lösung der vorstehend angegebenen Aufgaben ist für eine Vorrichtung, die als Hardware wenigstens eine zentrale Recheneinheit enthält, welche zentrale Recheneinheit zur Ausführung von Software und zum Erhalten von Daten von einem mit der Vorrichtung zusammenwirkenden externen Datenträger ausgebildet ist, darüber hinaus vorgesehen, dass eine Schaltung der oben angegebenen Art mit der zentralen Recheneinheit gekoppelt ist.

Durch die erfindungsgemäßen Merkmale wird erreicht, dass eine direkte Kommunikation bzw. ein direkter Datenaustausch zwischen der ersten Einheit und der zweiten Einheit unter Vermeidung eines Umwegs über eine zentrale Recheneinheit der Vorrichtung vorgenommen wird. Entsprechend den obigen Ausführungen ist die erste Einheit zum Überprüfen und/oder Autorisieren bzw. Identifizieren von Hardware und/oder Software der Vorrichtung beispielsweise wiederum durch einen Trusted Platform Module (TPM) gebildet, während die zweite Einheit zum Überprüfen und/oder Autorisieren des externen Datenträgers wiederum von einem Secure Application Module (SAM) gebildet sein kann. Dadurch, dass erfindungsgemäß ein direkter Datenaustausch bzw. eine direkte Kommunikation zwischen der ersten und zweiten Einheit und insbesondere zwischen den

zentralen Recheneinheiten der ersten und zweiten Einheit vorgesehen ist, kann nicht nur eine Vereinfachung dahingehend erzielt werden, dass für die Kommunikation zwischen den Einheiten bzw. Modulen nicht jeweils eine Verbindung mit der zentralen Recheneinheit der Vorrichtung erforderlich ist, wie dies gemäß dem Stand der Technik der Fall ist, sondern es kann beispielsweise auf ein aufwendiges gegenseitiges Überprüfen der einzelnen Module bzw. ein gegenseitiges Autorisieren zwischen den einzelnen Modulen verzichtet werden. Weiters ergibt sich erfindungsgemäß, dass bei Vorsehen eines direkten Datenaustauschs bzw. eines Kommunikations-Interfaces zwischen den zentralen Recheneinheiten der ersten Einheit und der zweiten Einheit die Möglichkeit einer Manipulation bzw. eines Angriffs auf ein derartiges Kommunikations-Interface, welches in einer gemeinsamen Schaltung integriert bzw. aufgenommen ist, stark gegenüber der Möglichkeit einer Manipulation bzw. eines Angriffs auf die Interfaces zwischen den einzelnen Modulen und der zentralen Recheneinheit vermindert werden kann. Für den direkten Datenaustausch zwischen der ersten Einheit und der zweiten Einheit kann auf ein sehr einfaches Kommunikationsprotokoll, wie beispielsweise das standardisierte I^2C-Protokoll, zurückgegriffen werden, um eine direkte Kommunikation zwischen den zentralen Recheneinheiten der ersten Einheit und der zweiten Einheit zu ermöglichen.

Gemäß den Maßnahmen des Anspruchs 2 ist der Vorteil erhalten, dass eine sichere gegenseitige Überprüfung der ersten Einheit und der zweiten Einheit zur Verfügung gestellt wird. Dies kann beispielsweise dadurch erfolgen, dass von der zentralen Recheneinheit eines Moduls eine Zufallszahl erzeugt und mit einem gemeinsamen Schlüssel verschlüsselt wird, worauf die verschlüsselte Zahl und eine neue Zufallszahl an das andere Modul übersandt wird. Falls vom zweiten Modul eine korrekte Verschlüsselung erkannt wird, wird von diesem neuerlich eine Verschlüsselung einer Zufallszahl mit dem gemeinsamen Schlüssel vorgenommen und diese Zufallszahl an das erste Modul zurück übermittelt, worauf wiederum ein Authentisieren bzw. Identifizieren des zweiten Moduls durch das erste Modul erfolgt. Durch den direkten Datenaustausch bzw. das Kommunikations-Interface zwischen der ersten Einheit und der zweiten Einheit ist eine entsprechend sichere direkte Kopplung zwischen der ersten Einheit und der zweiten Einheit realisiert, welche beiden Einheiten als aktive Komponenten ausgebildet sind.

Gemäß den Maßnahmen des Anspruchs 3 ist der Vorteil erhalten, dass ein wechselweises Überprüfen und Identifizieren zwischen der ersten Einheit und der zweiten

Einheit bzw. zwischen den unterschiedlichen Modulen bevor ein Überprüfen bzw. Identifizieren von Hardware und/oder Software oder von einem mit der Vorrichtung zusammenwirkenden Datenträger erfolgt, so dass sichergestellt wird, dass nicht eine der Einheiten bzw. eines der Module nach einem Eingriff in die zentrale Recheneinheit der Vorrichtung oder nach einem Eingriff in Daten eines externen Datenträgers manipuliert wurde.

Gemäß den Maßnahmen des Anspruchs 4 ist der Vorteil erhalten, dass in den einzelnen Einheiten bzw. Modulen vorgesehene Elemente bzw. Komponenten wenigstens teilweise durch die in direktem Datenaustausch bzw. in direkter Kommunikation stehenden beiden Einheiten gemeinsam genutzt werden, so dass der Aufwand für die Herstellung bzw. Ausbildung der einzelnen Einheiten bzw. Module reduziert werden kann.

Gemäß den Maßnahmen der Ansprüche 5 und 10 wird eine zusätzliche Erhöhung der Sicherheit bei dem Identifizieren und/oder Überprüfen geboten.

Gemäß den Maßnahmen der Ansprüche 6 und 13 wird der Einsatz von weit verbreiteten externen Datenträgern zur Verfügung gestellt.

Gemäß den Maßnahmen des Anspruchs 8 ist der Vorteil erhalten, dass entsprechend den Anforderungen an die erste Einheit und die zweite Einheit bzw. die einzelnen Module die unterschiedlichen erforderlichen Speicher getrennt zur Verfügung gestellt werden können.

Gemäß den Maßnahmen des Anspruchs 9 ist der Vorteil erhalten, dass gegebenenfalls eine gleiche bzw. ähnliche Funktion ausübende Komponenten der einzelnen Einheiten bzw. Module gemeinsam genutzt werden bzw. in einer einzigen Komponente kombiniert werden können, um dadurch den Aufwand für die Herstellung der erfindungsgemäßen Schaltung zu verringern bzw. zu minimieren.

Gemäß den Maßnahmen des Anspruchs 11 ist der Vorteil erhalten, dass der Aufwand für die Herstellung der erfindungsgemäßen Schaltung weiter verringert werden kann, da mit einer gemeinsamen zentralen Recheneinheit das Auslangen gefunden werden kann. Darüber hinaus wird durch Vorsehen einer gemeinsamen zentralen Recheneinheit, welche die Funktion der zentralen Recheneinheit sowohl der ersten Einheit als auch der zweiten Einheit ausübt, erreicht, dass mit einem gemeinsamen Interface mit der zu identifizierenden und/oder zu überprüfenden Hardware und/oder Software das Auslangen gefunden werden kann, so dass wiederum eine Reduktion erforderlicher Komponenten

erzielbar ist. Durch das Vorsehen einer kombinierten bzw. gemeinsamen zentralen Recheneinheit wird darüber hinaus ermöglicht, dass Angriffe bzw. Manipulationen an dem Interface bzw. im Zusammenhang mit dem direkten Datenaustausch zwischen der ersten Einheit und der zweiten Einheit praktisch nicht möglich sind.

Gemäß den Maßnahmen des Anspruchs 15 ist der Vorteil erhalten, dass die Möglichkeiten zur Manipulation und/oder für einen Angriff auf die Verbindung bzw. das Interface zwischen der erfindungsgemäßen Schaltung und der zentralen Recheneinheit der damit auszurüstenden Vorrichtung weiter herabgesetzt werden, da durch die Integration der erfindungsgemäßen Schaltung in die zentrale Recheneinheit der damit auszurüstenden Vorrichtung auch die Kommunikation bzw. ein hierfür erforderliches Interface unmittelbar in die zentrale Recheneinheit der mit der erfindungsgemäßen Schaltung auszurüstenden Vorrichtung integriert wird, wobei ein derartiges integriertes Interface bedeutend schwieriger anzugreifen bzw. zu manipulieren ist, da dies beispielsweise eine Öffnung der zentralen Recheneinheit erfordern würde, was praktisch nicht möglich ist.

Die vorstehend angeführten Aspekte und weitere Aspekte der Erfindung gehen aus den nachfolgend beschriebenen Ausführungsbeispielen hervor und sind anhand dieser Ausführungsbeispiele erläutert.

Die Erfindung wird im Folgenden anhand von in den Figuren dargestellten Ausführungsbeispielen beschrieben, auf welche die Erfindung aber nicht beschränkt ist.

Die Figur 1 zeigt ein Blockdiagramm einer ersten Ausführungsform einer erfindungsgemäßen Schaltung zur Durchführung eines erfindungsgemäßen Verfahrens.

Die Figur 2 zeigt schematisch ein Flußdiagramm, gemäß welchem die in direktem Datenaustausch bzw. in direkter Verbindung stehende erste Einheit und zweite Einheit eine gegenseitige Überprüfung vornehmen.

Die Figur 3 zeigt analog wie die Figur 1 eine erfindungsgemäße Schaltung mit einer abgewandelten Ausführungsform.

Die Figur 4 zeigte eine erfindungsgemäße Schaltung gemäß einer weiteren abgewandelten Ausführungsform, wobei die zentrale Recheneinheit der ersten Einheit und der zweiten Einheit in einer gemeinsamen zentralen Recheneinheit kombiniert sind.

Die Figur 5 zeigt in Form eines Blockdiagramms eine erfindungsgemäße

Vorrichtung, welche mit einer erfindungsgemäßen Schaltung gekoppelt ist.

Die Figur 6 zeigt ähnlich wie die Figur 5 eine erfindungsgemäße Vorrichtung mit einer abgewandelten Ausführungsform, wobei die erfindungsgemäße Schaltung in die zentrale Recheneinheit der Vorrichtung integriert ist.

Die Figur 1 zeigt allgemein ein Blockdiagramm einer Schaltung, insbesondere einer integrierten Schaltung 1, wobei eine erste Einheit E1 und eine zweite Einheit E2 zum Identifizieren und/oder Autorisieren von Hardware und/oder Software einer Vorrichtung sowie zum Identifizieren und/oder Autorisieren von einem Datenträger (9) in einem direkten Datenaustausch miteinander stehen.

Die erste Einheit E1 ist im wesentlichen durch ein Trusted Platform Module TPM mit einer zentralen Recheneinheit 2 gebildet, welches Modul TPM mit einem ROM 3 und einem RAM 4 und einem nicht flüchtigen Speicher 5, welcher beispielsweise von einem EEPROM oder Flash-Memory gebildet sein kann, zusammenwirkt, wie dies schematisch in Figur 1 dargestellt ist. Darüber hinaus ist eine Verschlüsselungsmaschine 6 für die erste Einheit E1 (TPM) und ein Interface 7, wie beispielsweise ein Low Pin Count-Interface, kurz LPC, zu einer zentralen Recheneinheit 8 einer in Figur 1 nicht im Detail dargestellten Vorrichtung 23 angegeben.

Die durch einen Trusted Platform Module TPM gebildete erste Einheit E1 dient zum Überprüfen bzw. Identifizieren und/oder Autorisieren von Hardware und/oder Software der zentralen Recheneinheit 8 einer Vorrichtung 23, welche Vorrichtung 23 beispielsweise durch einen PC, einen CD-Player, ein Fernsehgerät, ein Mobiltelefon oder einen Personal-Digital-Assistent gebildet sein kann.

Zum Überprüfen und/oder Identifizieren von Autorisierungsdaten des schematisch dargestellten Datenträgers 9, welcher beispielsweise von einer SmartCard gebildet ist, besteht die insbesondere von einem Secure Application Module SAM gebildete zweite Einheit E2 aus einer zentralen Recheneinheit 10 der zweiten Einheit E2, wobei ähnlich wie bei der ersten Einheit E1 wiederum ein ROM 11 und ein RAM 12 und wenigstens ein nicht flüchtiger Speicher 13 vorgesehen ist. Für eine Verschlüsselung von Daten bzw. Informationen ist auch für die zweite Einheit E2 eine Verschlüsselungsmaschine 14 vorgesehen. Für ein Kommunizieren mit der zentralen

Recheneinheit 8 der Vorrichtung 23 ist auch für die zweite Einheit E2 ein Interface 15 vorgesehen. Für ein Kommunizieren mit dem externen Datenträger 9 ist weiters ein Interface 16 vorgesehen, welches beispielsweise durch ein ISO 7816-Interface und/oder ein ISO 14443-Interface und/oder ein USB-Interface gebildet sein kann.

Das Identifizieren und/oder Überprüfen von Hardware und/oder Software der Vorrichtung 23 als auch von dem Datenträger 9 erfolgt hierbei allgemein derart, dass sowohl von der Hardware und/oder Software als auch von dem externen Datenträger 9 jeweils individuelle Autorisierungsdaten an die erste Einheit E1 bzw. die zweite Einheit E2 unter Zwischenschaltung der entsprechenden Interfaces 7 bzw. 16 übersandt werden, wobei in der jeweiligen zentralen Recheneinheit 2 bzw. 10, insbesondere nach einem Ver- bzw. Entschlüsseln in den Verschlüsselungseinrichtungen 6 bzw. 14 ein Vergleich mit ersten Prüfdaten bzw. zweiten Prüfdaten erfolgt, wonach eine Autorisierung sowohl der Hardware und/oder Software durch die zentrale Recheneinheit 2 als auch des externen Datenträgers 9 durch die zentrale Recheneinheit 10 erfolgt.

Darüber hinaus ist in dem in Figur 1 dargestellten Blockdiagramm ein weiteres Kommunikations-Interface 17 vorgesehen, welches ein direktes Kommunizieren bzw. Verbinden oder ein direktes Datenaustauschen zwischen der ersten Einheit E1, welche durch das TPM gebildet ist, und der zweiten Einheit E2, welche durch das SAM gebildet ist, ermöglicht.

Durch ein derartiges, direktes Datenaustauschen bzw. ein direktes Kommunizieren über das Interface 17 zwischen der ersten Einheit E1 und der zweiten Einheit E2 kann die Möglichkeit eines Manipulierens bzw. eines Eingreifens in den Vorgang des Datenaustauschens zwischen den beiden Einheiten E1 und E2 praktisch vollkommen ausgeschlossen werden. Für den über das Interface 17 zur Verfügung gestellten Kommunikationskanal im Inneren der Schaltung 1 kann ein sehr einfaches Kommunikationsprotokoll, beispielsweise das standardisierte I^2C-Protokoll verwendet werden, um das direkte Kommunizieren zwischen der zentralen Recheneinheit 2 der ersten Einheit E1 (nachfolgend kurz TPM genannt) und der zentralen Recheneinheit 10 der zweiten Einheit E2 (nachfolgend kurz SAM genannt) zu ermöglichen. Das direkte und einfache Kommunizieren ermöglicht ein direktes bzw. gegenseitiges Autorisieren bzw. Identifizieren der ersten Einheit E1 als auch der zweiten Einheit E2, wobei beispielsweise ein gemeinsamer Schlüssel verwendet wird, welcher in den ROMs 3 bzw. 11 gespeichert

ist.

Das Autorisieren bzw. das Identifizieren der ersten Einheit E1 (TPM) sowie der zweiten Einheit E2 (SAM) wird anhand des in Figur 2 schematisch dargestellten Flußdiagramms nachfolgend näher erläutert.

In einem ersten Schritt S1 erfolgt ein Rücksetzen der in Figur 1 gezeigten Schaltung 1, wonach in einem Schritt S2 von dem SAM über das Interface 17 eine Zufallszahl an die zentrale Recheneinheit 2 des TPM gesandt wird. Mit Hilfe der Verschlüsselungsmaschine 6 des TPM und eines für das SAM und des TPM gemeinsam definierten Schlüssels, der im ROM 3 gespeichert ist, erfolgt in einem Schritt S3 ein Verschlüsseln der Zufallszahl, welche in einem Schritt S4 über das Interface 17 an die CPU bzw. die zentrale Recheneinheit 10 des SAM gemeinsam mit einer neuen Zufallszahl, die in den TPM erzeugt wurde, gesandt wird.

In einem Schritt S5 erfolgt bei dem SAM ein Überprüfen, ob durch das TPM ein korrektes Verschlüsseln unter Verwendung des gemeinsamen Schlüssels erfolgte, so dass bewiesen ist, dass bei dem TPM tatsächlich der gemeinsame Schlüssel zur Anwendung gekommen ist. Wenn das Resultat der Überprüfung der Verschlüsselung negativ ist, wird in einem Schritt S6 das SAM außer Betrieb gesetzt.

Wenn das Resultat der Überprüfung in Schritt S5 positiv ist, erfolgt bei dem SAM in einem Schritt S7 ein Verschlüsseln der neuen Zufallszahl mit dem gemeinsam Schlüssel unter Verwendung der Verschlüsselungsmaschine 14, worauf in einem Schritt S8 die verschlüsselte neue Zufallszahl über das Interface 17 an die CPU bzw. die zentrale Recheneinheit 2 des TPM gesendet wird.

In einem Schritt S9 erfolgt bei dem TPM in Analogie zu der Überprüfung bei dem SAM ein Überprüfen, ob ein korrektes Verschlüsseln durch die zentrale Recheneinheit 2 des SAM erfolgt. Falls die Verschlüsselung nicht korrekt ist, wird in einem Schritt S10 das TPM ausgeschaltet, während bei erfolgreicher Überprüfung in einem Schritt S11 das TPM eingeschaltet bzw. aktiviert wird bzw. bleibt.

Es sei an dieser Stelle erwähnt, dass die Prüfvorgänge durch das SAM und das TPM auch in anderer Aufeinanderfolge durchgeführt werden können.

Der Vorteil des unmittelbaren und direkten Verifizierens bzw. Autorisierens zwischen der ersten Einheit E1 und der zweiten Einheit E2 unter Verwendung des in Figur 1 dargestellten, direkten Kommunikations-Interfaces 17 liegt darin, dass ohne

Zwischenschaltung beispielsweise einer externen, zentralen Recheneinheit 8, wie dies gemäß dem bekannten Stand der Technik der Fall ist, direkt ein gegenseitiges Überprüfen zwischen dem SAM und dem TPM über eine sehr einfache direkte Verbindung vorgenommen werden kann.

Im Gegensatz zum Stand der Technik ist weiters der Vorteil erhalten, dass sowohl die erste Einheit E1, welche in diesem Fall durch ein TPM gebildet ist, als auch die zweite Einheit E2, welche in diesem Fall durch ein SAM gebildet ist, aktive Komponenten darstellen, da über den direkten Datenaustausch bzw. die direkte Kommunikation über das Interface 17 zwischen der ersten Einheit E1 und der zweiten Einheit E2 beispielsweise ein wechselweises Überprüfen und/oder Identifizieren bzw. Autorisieren zwischen der ersten Einheit E1 und der zweiten Einheit E2 vorgenommen werden kann.

Bei der Ausführungsform gemäß der Figur 3 ist vorgesehen, dass die zentrale Recheneinheit 2 bzw. CPU des TPM als auch die zentrale Recheneinheit 10 bzw. CPU des SAM über das direkte Kommunikations-Interface 17 verbunden sind. Im Gegensatz zu der Ausbildung gemäß der Figur 1 ist jedoch in der Figur 3 veranschaulicht, dass die zentralen Recheneinheiten 2 bzw. 10 jeweils auf ein gemeinsames ROM 18 und ein gemeinsames RAM 19 und einen gemeinsamen nicht flüchtigen Speicher 20 zugreifen. Es lassen sich somit im Vergleich mit der Figur 1 die für die Schaltung 1 erforderlichen Elemente reduzieren, so dass eine vereinfachte Ausbildung erhalten ist. Darüber hinaus erfolgt durch Vorsehen der gemeinsamen Elemente 18, 19 und 20 auch eine entsprechende Vereinfachung und Abgleichung der in den einzelnen Elementen 18, 19 und 20 gespeicherten Daten.

Wie bei der Ausführungsform gemäß Figur 1 ist auch bei der Ausbildung gemäß Figur 3 eine Verschlüsselungsmaschine 6 bzw. 14 für die zentralen Recheneinheiten 2 bzw. 10 vorgesehen. Ähnlich zu der Ausbildung gemäß Figur 1 sind darüber hinaus Interfaces 7 und 15 für die Kommunikation mit der zentralen Recheneinheit bzw. CPU 8 der Vorrichtung 23 angedeutet, während die CPU 10 des SAM über das Interface 16 eine Kommunikation mit einem externen Datenträger, beispielsweise einer SmartCard, ermöglicht ist.

Es kann erwähnt werden, dass abweichend von der Ausführungsform gemäß der Figur 3 nicht sämtliche der Elemente 18, 19 und 20 von beiden zentralen Recheneinheiten 2 bzw. 10 geteilt werden müssen, sondern dass gegenüber der

Ausführungsform gemäß Figur 1 beispielsweise lediglich durch Vorsehen eines gemeinsamen RAM 19 eine entsprechende Vereinfachung erzielbar ist.

Bei der in der Figur 4 dargestellten weiter abgewandelten Ausführung ist vorgesehen, dass anstelle der getrennten Recheneinheiten 2 bzw. 10 für das TPM als auch das SAM mit einer kombinierten bzw. gemeinsamen CPU 21 für das nunmehr mit SM bezeichnete Sicherheitsmodul bzw. Security Module das Auslangen gefunden werden kann. Die CPU 21 des Sicherheitsmoduls SM erfüllt sämtliche Funktionen der zentralen Recheneinheit bzw. CPU 2 des TPM als auch der CPU 10 des SAM. In der Figur 4 ist angedeutet, dass die kombinierte CPU 21 wiederum mit einer Verschlüsselungsmaschine 14 entsprechend der Verschlüsselungsmaschine des getrennten SAM der vorangehenden Ausführungsformen als auch mit einer Verschlüsselungsmaschine 6 entsprechend der Verschlüsselungsmaschine 6 des TPM der vorangehenden Ausführungsformen zusammenwirkt. Ähnlich wie bei der Ausführungsform gemäß der Figur 3 sind insbesondere unter Berücksichtigung der Tatsache, dass nur mehr eine kombinierte zentrale Recheneinheit bzw. CPU 21 vorgesehen ist, ein gemeinsames ROM 18 und ein gemeinsames RAM 19 und wenigstens ein gemeinsamer nicht flüchtiger Speicher 20 vorgesehen.

Durch die Kombination der zentralen Recheneinheiten des TPM und des SAM in eine gemeinsame zentrale Recheneinheit 21 kann auch mit einem einzigen Interface 22 für eine Verbindung bzw. für ein Kommunizieren mit der zentralen Recheneinheit 8 das Auslangen gefunden werden. Für ein Kommunizieren mit einem externen Datenträger 9 ist wiederum das Interface 16 vorgesehen.

Das für einen direkten Datenaustausch bzw. ein direktes Kommunizieren zwischen der ersten Einheit E1 und der zweiten Einheit E2 vorgesehene Kommunikations-Interface 17 der in den Figuren 1 und 3 dargestellten Ausführungsformen ist bei der in Figur 4 dargestellten Ausführungsform direkt in die kombinierte CPU 21 des Sicherheitsmoduls SM integriert. Durch eine derartige Bereitstellung einer kombinierten bzw. gemeinsamen CPU 21 läßt sich somit die Sicherheit der Schaltung 1 gegenüber einer Manipulation bzw. einem Eingriff weiter erhöhen, da ein direkter Eingriff in eine CPU 21 üblicherweise viel schwieriger vorgenommen werden kann, als ein Eingriff im Bereich eines Interface zwischen einzelnen Elementen einer Schaltung.

Darüber hinaus ist ersichtlich, dass die Anzahl der für die Schaltung 1

erforderlichen Bauteile weiter reduziert werden kann, da beispielsweise lediglich ein Interface für die Verbindung mit der zentralen Recheneinheit 8 erforderlich ist und auch wenigstens ein Teil der Funktionalitäten der jeweiligen zentralen Recheneinheit des SAM bzw. des TPM in der kombinierten CPU 21 des Sicherheitsmoduls SM nicht entsprechend mehrfach in der Ausführungsform gemäß der Figur 4 vorgesehen werden muss.

Die Figur 5 zeigt eine Kopplung der in den vorangehenden Ausführungsbeispielen gezeigten Schaltung 1 mit der zentralen Recheneinheit bzw. CPU 8 der Vorrichtung 23 Die in der Figur 5 angedeutete Schaltung 1 kann eine der in den Figuren 1, 3 bzw. 4 dargestellten Ausführungsformen sein, so dass in jedem Fall davon auszugehen ist, dass im Gegensatz zum Stand der Technik, bei welchem ein getrenntes SAM zum Überprüfen eines externen Datenträgers 9 als auch ein getrenntes TPM zum Überprüfen bzw. Identifizieren der zentralen Recheneinheit 8 vorgesehen sind, eine direktes Kommunizieren zwischen dem TPM und dem SAM ermöglicht bzw. vorgesehen ist. Die Verbindung zwischen der Schaltung 1 und der zentralen Recheneinheit 8 kann, wie dies bei den Ausführungsformen gemäß den Figuren 1 und 3 der Fall ist, über getrennte Verbindungen bzw. über getrennte Interfaces zu der zentralen Recheneinheit 8 vorgesehen sein, während bei der Verwendung einer Schaltung 1 gemäß der Figur 4 lediglich ein Interface 22 für die Verbindung bzw. Kommunikation zwischen der Schaltung 1 und der zentralen Recheneinheit 8 vorgesehen ist.

In der Figur 5 ist weiters angedeutet, dass zusätzlich externe Daten aus einer externen Datenquelle 24 der zentralen Recheneinheit 8 als auch innerhalb der Vorrichtung 23 bereits enthaltene Daten aus einer internen Datenquelle 25 dieser CPU 8 zur Verfügung gestellt werden können.

Bei der abgewandelten Ausführungsform gemäß Figur 6 ist ersichtlich bzw. angedeutet, dass eine Schaltung 1, welche das Sicherheitsmodul SM gemäß Figur 4 enthält, in die zentrale Recheneinheit bzw. CPU 8 integriert bzw. derart mit ihr gekoppelt ist, dass eine Verbindung zwischen dem Sicherheitsmodul SM und der zentralen Recheneinheit 8 über ein in die zentrale Recheneinheit 8 integriertes Interface vorgenommen wird. Es lassen sich derart die Möglichkeiten einer Manipulation bzw. eines Eingriffs in die Kommunikation bzw. Verbindung zwischen der Schaltung 1 und der zentralen Recheneinheit 8 gegenüber der in Figur 5 dargestellten Ausführungsform weiter verringern, so dass insgesamt die Sicherheit der Kommunikation beim Überprüfen bzw. Identifizieren

oder Autorisieren weiter erhöht wird.

Es kann erwähnt werden, dass anstelle der in den Ausführungsbeispielen beispielhaft genannten SmartCard als externer Datenträger 9 auch beispielsweise ein Tag bzw. ein intelligentes Etikett bzw. Label verwendet werden kann.

Es kann weiters erwähnt werden, dass neben den oben genannten Beispielen für die Vorrichtung 23, welche sich insbesondere auf Konsumgüter bezogen haben, die Vorrichtung 23 beispielsweise durch ein Zugangskontrolleinrichtung oder eine gesicherte Anlagensteuereinrichtung realisiert sein kann, wobei für derartige Vorrichtungen ein Überprüfen der Unversehrtheit der Hardware und/oder Software oder ein Identifizieren derselben als auch ein Überprüfen oder Identifizieren eines Datenträgers von großer Wichtigkeit sind.

Es kann weiters erwähnt werden, dass beispielsweise der Datenträger 9 für eine kontaktlose Kommunikation vorgesehen sein kann.

Weiters kann erwähnt werden, dass neben einer Aufnahme bzw. Integration einer Schaltung 1 in eine Vorrichtung 23 eine derartige Schaltung 1 auch gegebenenfalls in dem entsprechenden Datenträger 9 zum Überprüfen oder Identifizieren bzw. Autorisieren seiner Hardware oder seiner Software bzw. zum Identifizieren und/oder Überprüfen von einer mit dem Datenträger 9 zusammenwirkenden Vorrichtung 23 integriert sein kann.

Es kann weiters erwähnt werden, dass anstelle des in den vorstehend beschriebene Ausführungsbeispielen für die zweite Einheit E2 genannten SAM auch andere Module bzw. Schaltungen verwendet werden können, welche eine Identifizierung oder Autorisierung von Autorisierungsdaten eines externen Datenträgers, beispielsweise einer SmartCard, ermöglichen. Beispielsweise kann zum Realisieren der Funktionalität der zweiten Einheit auch die Funktionalität eines sogenannten Readers angewendet werden, der im Zusammenhang mit einer Wegfahrsperre bei Kraftfahrzeugen bekannt ist, wobei die Funktionalität des Readers zum Autorisieren des elektronischen Autoschlüssels dient. Als ein weiteres Beispiel kann die Funktionalität einer Softwareroutine angeführt werden, die auf einem PC abgearbeitet wird und nur dann eine Applikation oder den PC zur Benutzung durch einen Benutzer verfügbar macht, wenn die Software einen an dem Druckeranschluss des PC oder dem USB-Anschluss des PC angeschlossenen elektronischen Schlüssel autorisiert, der auch unter dem Begriff „Hardware-Tongle" bekannt ist und der die Funktion des Datenträgers übernimmt.

Es kann erwähnt werden, dass anstelle des in den vorstehend erörterten Ausführungsbeispielen für die erste Einheit genannten TPM auch eine Funktionalität eines sogenannten „Trusted Computer Platform Alliance Chip“ oder eines „Trusted Computer Group Chip“ vorgesehen sein kann. Weiters kann zum Realisieren der Funktion der ersten Einheit auch die Funktionalität eines von der Firma ATMEL hergestellten sogenannten „Security Chip" oder „Security Module" zur Anwendung kommen, wie sie gegenwärtig bei Laptops der Firma IBM zum Einsatz kommen.

Es sei weiters erwähnt, das anstelle des gemeinsamen Schlüssels auch ein Schlüsselpaar zum Einsatz kommen kann.

Patentansprüche:

1. Verfahren zum Identifizieren und/oder Überprüfen von Hardware und/oder Software einer Vorrichtung (23) und von einem Datenträger (9), der zum Zusammenwirken mit der Vorrichtung vorgesehen ist, umfassend die folgenden Schritte:

Übertragen von ersten Autorisierungsdaten der Hardware und/oder Software an eine erste Einheit (E1),

Vergleichen der an die erste Einheit (E1) übertragenen ersten Autorisierungsdaten der Hardware und/oder Software mit in der ersten Einheit (E1) gespeicherten ersten Prüfdaten,

Autorisieren der Hardware und/oder Software nach Feststellen einer Übereinstimmung zwischen den von der Hardware und/oder Software zur Verfügung gestellten ersten Autorisierungsdaten und den in der ersten Einheit (E1) gespeicherten ersten Prüfdaten,

Übertragen von zweiten Autorisierungsdaten eines Datenträgers (9) an eine zweite Einheit (E2),

Vergleichen der zweiten Autorisierungsdaten in der zweiten Einheit (E2) mit in der zweiten Einheit (E2) gespeicherten zweiten Prüfdaten,

Autorisieren des Datenträgers (9) bei einer Übereinstimmung zwischen den zweiten Autorisierungsdaten und den in der zweiten Einheit (E2) gespeicherten zweiten Prüfdaten,

wobei ein direktes Datenaustauschen zwischen der ersten Einheit (E1) und der zweiten Einheit (E2) vorgenommen wird.

2. Verfahren gemäß Anspruch 1,

wobei das direkte Datenaustauschen zwischen der ersten Einheit (E1) und der zweiten Einheit (E2) eine Übermittlung von verschlüsselten Daten und ein Vergleichen und/oder Entschlüsseln von zwischen der ersten Einheit (E1) und der zweiten Einheit (E2) übermittelten Daten umfasst.

3. Verfahren gemäß Anspruch 1 oder 2,

wobei das Datenaustauschen zwischen der ersten Einheit (E1) und der zweiten Einheit (E2) vor einer Identifizierung und/oder Überprüfung von ersten Autorisierungsdaten der Hardware und/oder Software und von zweiten Autorisierungsdaten des Datenträgers (9) vorgenommen wird.

4. Verfahren nach einem der Ansprüche 1, 2 oder 3,
wobei eine zentrale Recheneinheit (2) der ersten Einheit (E1) und eine zentrale Recheneinheit (10) der zweiten Einheit (E2) gemeinsam auf wenigstens einen ROM-Speicher (18), einen RAM-Speicher (19) und/oder einen nicht-flüchtigen Speicher (20) zugreifen.

5. Verfahren nach einem der Anspräche 1 bis 4,
wobei in der ersten Einheit (E1) und in der zweiten Einheit (E2) ein Verschlüsseln (6, 14) der ersten Autorisierungsdaten und der zweiten Autorisierungsdaten vorgenommen wird.

6. Verfahren nach einem der Ansprüche 1 bis 5,
wobei die zweiten Autorisierungsdaten von einer den Datenträger (9) realisierenden SmartCard oder einem Tag oder einem Label erhalten werden.

7. Schaltung zum Identifizieren und/oder Überprüfen von Hardware und/oder Software einer Vorrichtung (23) und von einem Datenträger (9), der zum Zusammenwirken mit der Vorrichtung vorgesehen ist, umfassend:

eine erste Einheit (E1) zum Identifizieren und/oder Überprüfen der Hardware und/oder Software der Vorrichtung, enthaltend eine zentrale Recheneinheit (2) und wenigstens einen Speicher (3, 4, 5, 18, 19, 20) und ein Interface (7, 22) zu der zu identifizierenden und/oder zu überprüfenden Hardware und/oder Software, und

eine zweite Einheit (E2), enthaltend eine zentrale Recheneinheit (10) und wenigstens einen Speicher (11, 12, 13, 18, 19, 20) und ein Interface (16) zu einem externen Datenträger (9) sowie ein Interface (15) zu der Hardware und/oder Software,

worin ein Kommunikations-Interface (17) zwischen den zentralen Recheneinheiten (2, 10) der ersten Einheit (E1) und der zweiten Einheit (E2) vorgesehen ist.

8. Schaltung nach Anspruch 7,
wobei die Speicher der ersten Einheit (E1) und der zweiten Einheit (E2) von einem ROM-Speicher (3, 11, 18) und einem RAM-Speicher (4, 12, 19) und/oder einem nicht-flüchtigen Speicher (5, 13, 20) gebildet sind.

9. Schaltung nach Anspruch 7 oder 8,
wobei die ROM-Speicher und/oder die RAM-Speicher und/oder die nicht-flüchtigen Speicher der ersten Einheit (E1) und der zweiten Einheit (E2) jeweils zu einem gemeinsamen ROM-Speicher (18) und/oder einem gemeinsamen RAM-Speicher (19)

und/oder einem gemeinsamen nicht-flüchtigen Speicher (20) kombiniert sind.

10. Schaltung nach einem der Ansprüche 7 bis 9,
wobei die erste Einheit (E1) und die zweite Einheit (E2) jeweils eine Verschlüsselungseinrichtung (6, 14) enthalten.

11. Schaltung nach einem der Ansprüche 7 bis 10,
wobei die zentrale Recheneinheit der ersten Einheit (E1) und die zentrale Recheneinheit der zweiten Einheit (E2) zu einer gemeinsamen zentralen Recheneinheit (21) kombiniert sind, welche gemeinsame zentrale Recheneinheit (21) das Kommunikations-Interface integriert aufweist, und
wobei die gemeinsame zentrale Recheneinheit (21) mit einem Interface (22) mit der zu identifizierenden und/oder zu überprüfenden Hardware und/oder Software verbunden ist.

12. Schaltung nach einem der Ansprüche 7 bis 11,
wobei das Interface (16) zu dem externen Datenträger (9) für eine kontaktlose Kommunikation mit dem externen Datenträger (9) ausgebildet ist.

13. Schaltung nach einem der Ansprüche 7 bis 12,
wobei der externe Datenträger (9) von einer SmartCard oder einem Tag oder einem Label gebildet ist.

14. Vorrichtung, die als Hardware wenigstens eine zentrale Recheneinheit (8) enthält, welche zentrale Recheneinheit (8) zum Ausführen von Software und zum Erhalten von Daten von einem mit der Vorrichtung zusammenwirkenden externen Datenträger (9) ausgebildet ist, wobei eine Schaltung (1) nach einem der Ansprüche 7 bis 13 mit der zentralen Recheneinheit (8) gekoppelt ist.

15. Vorrichtung nach Anspruch 14,
wobei die zentrale Recheneinheit (8) der Vorrichtung (23) über ein in der zentralen Recheneinheit (8) der Vorrichtung integriertes Interface mit der in die zentrale Recheneinheit (8) integrierten Schaltung (1, SM) gekoppelt ist.

Zusammenfassung:

Verfahren und Schaltung zum Identifizieren und/oder Überprüfen von Hardware und/oder Software einer Vorrichtung und von einem mit der Vorrichtung zusammenwirkenden Datenträger

Bei einem Verfahren und einer Schaltung zum Identifizieren und/oder Überprüfen der Hardware und/oder Software einer Vorrichtung und von einem mit der Vorrichtung zusammenwirkenden Datenträger, beispielsweise einer SmartCard, ist vorgesehen, dass eine erste Einheit (E1) zum Überprüfen der Hardware und/oder Software der Vorrichtung, insbesondere ein Trusted Platform Module (TPM), als auch eine zweite Einheit (E2) zum Überprüfen und/oder Identifizieren bzw. Autorisieren von dem externen Datenträger, insbesondere ein Secure Application Module (SAM), für einen direkten Datenaustausch über ein Kommunikations-Interface (17) der zentralen Recheneinheiten (2, 10) gekoppelt sind, um die Möglichkeiten eines Eingriffs bzw. einer Manipulation zu reduzieren bzw. auszuschließen.

(Figur 1)

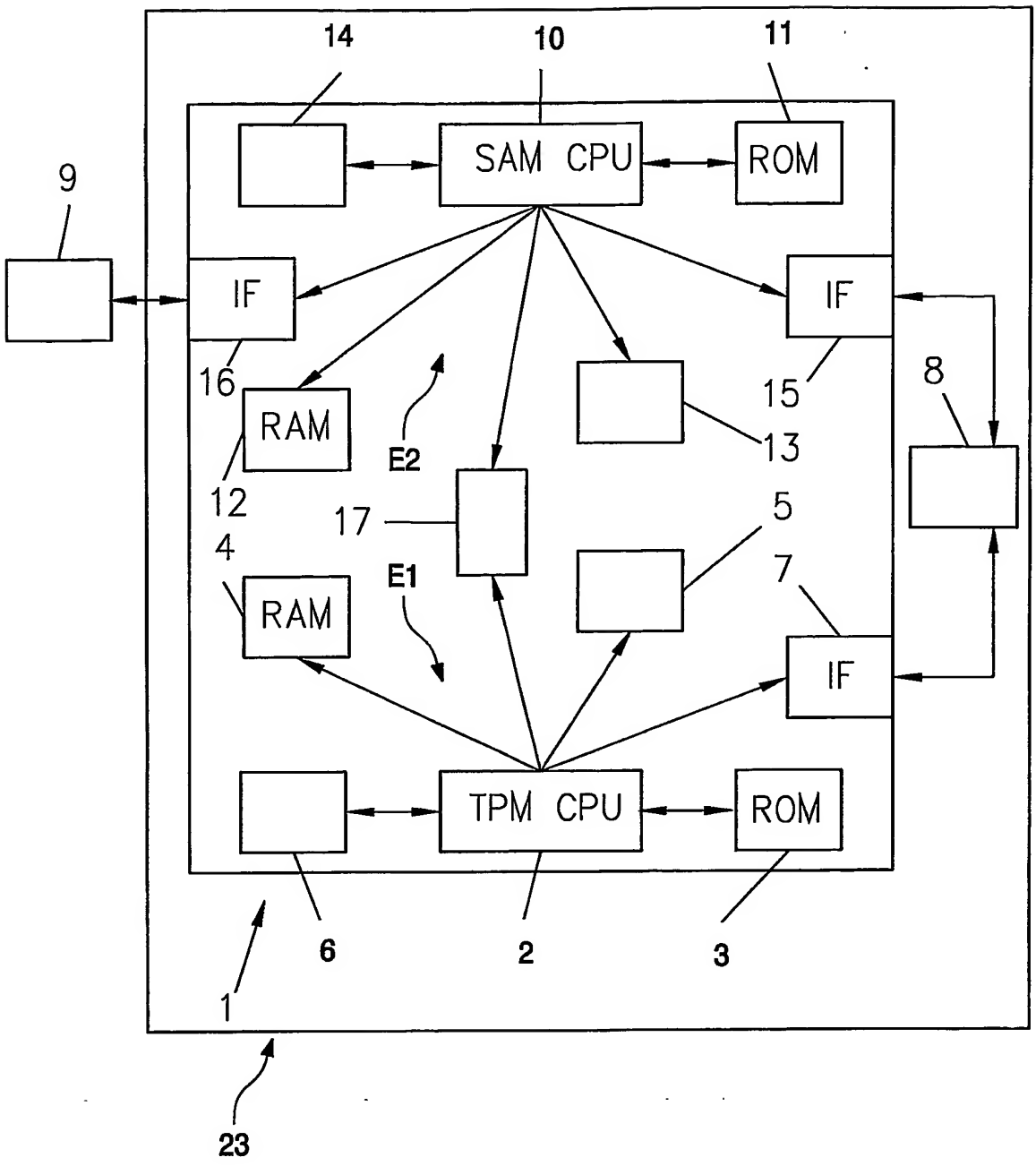
14
10
11
SAM CPU
ROM
9
IF
IF
16
RAM
E2
15
8
13
12
17
5
4
E1
7
RAM
IF
TPM CPU
ROM
6
2
3
1
23

FIG. 1

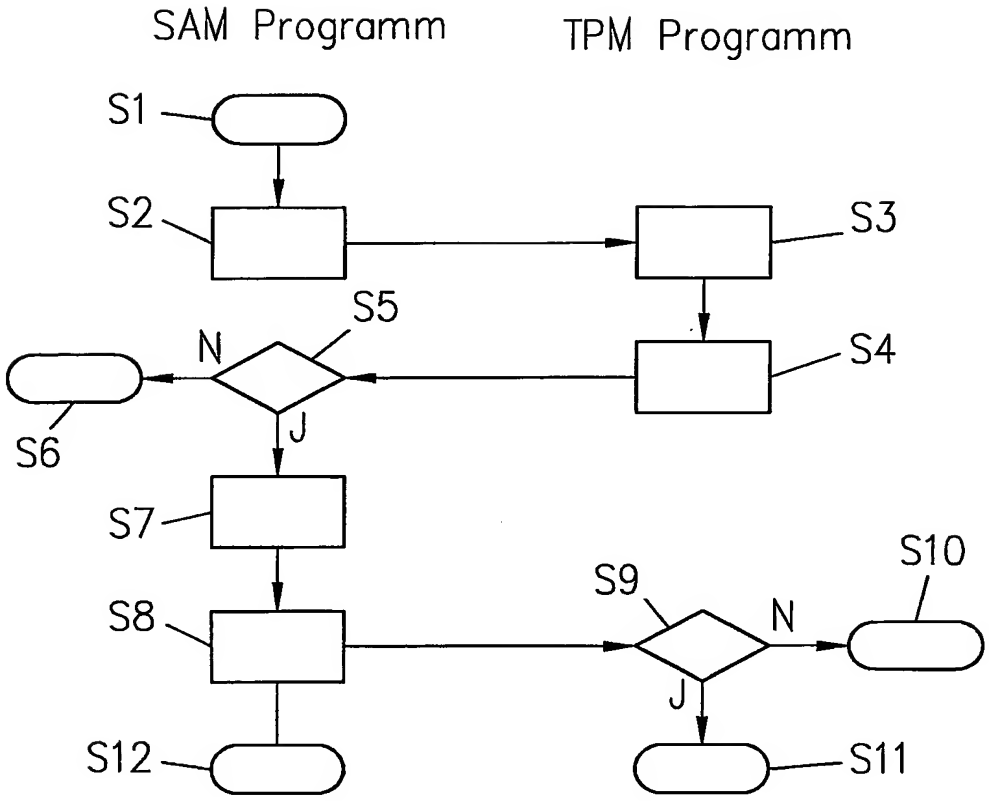
SAM Programm
TPM Programm
S1
S2
S3
S4
S5
N
J
S6
S7
S8
S9
N
S10
J
S11
S12

FIG. 2

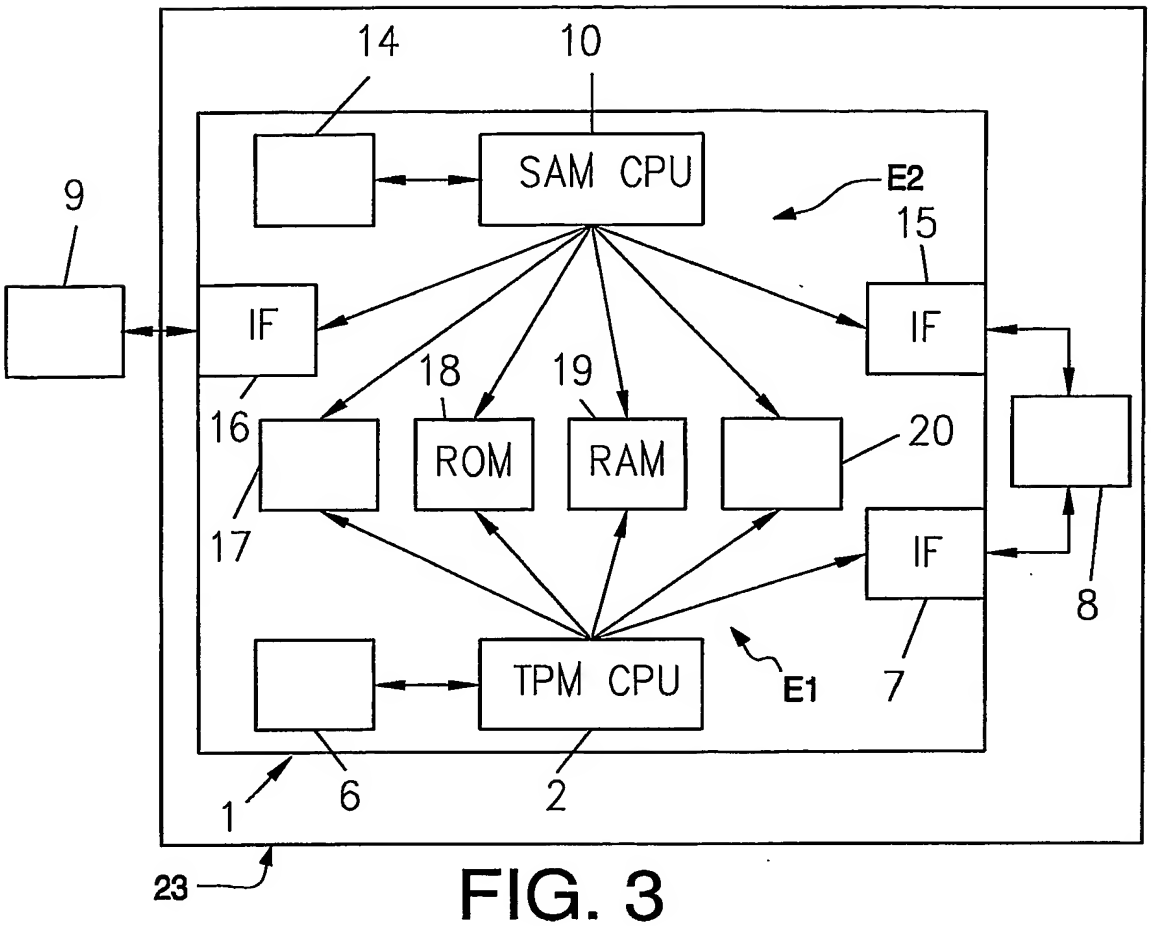
14
10
SAM CPU
E2
9
15
IF
IF
18
19
16
ROM
RAM
20
17
IF
8
TPM CPU
E1
7
1
6
2
23

FIG. 3

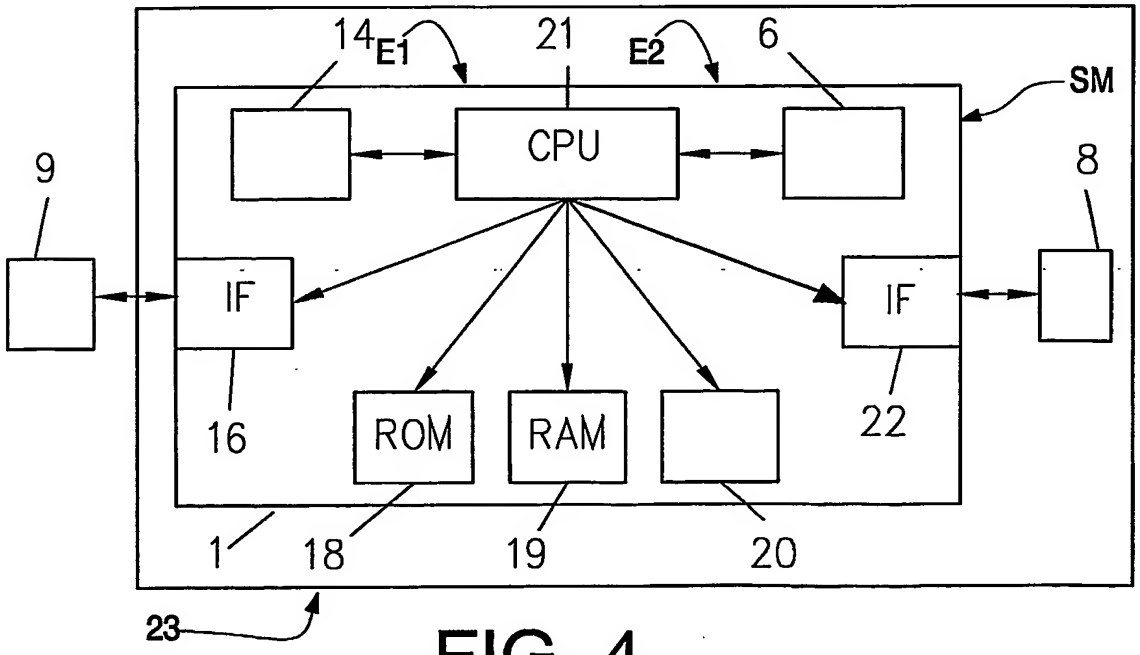
14
E1
21
E2
6
SM
CPU
9
8
IF
IF
16
ROM
RAM
22
1
18
19
20
23

FIG. 4

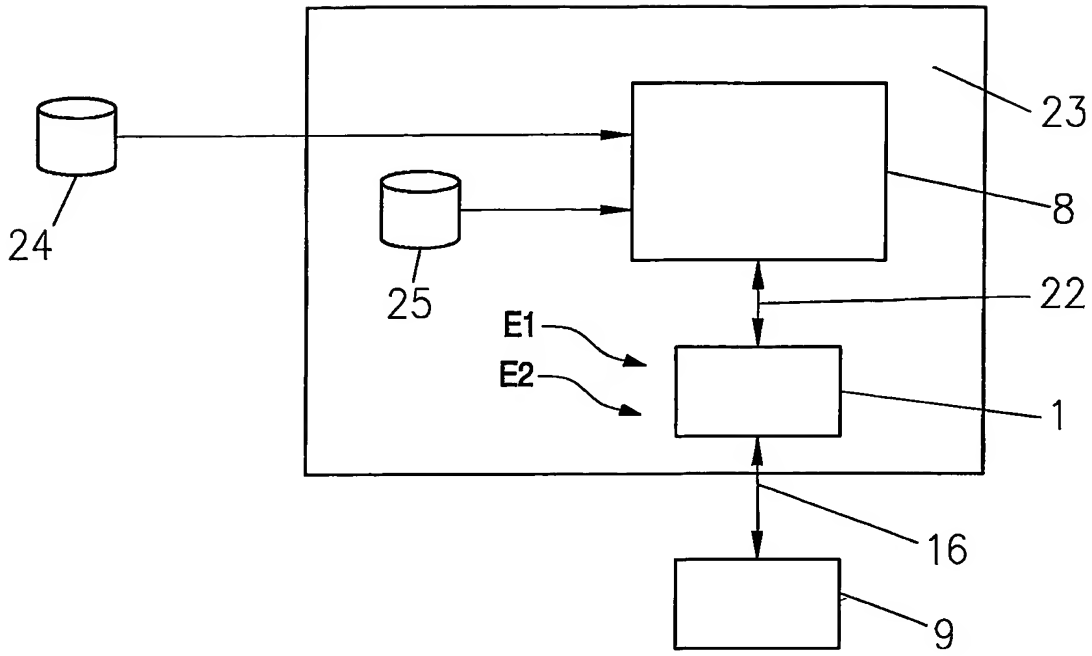

FIG. 5

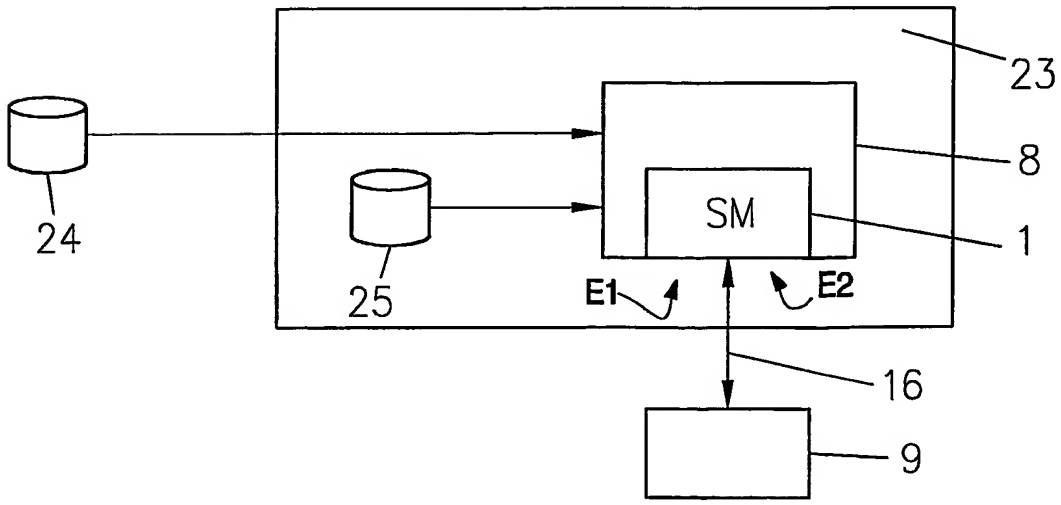

FIG. 6